Entendendo a espionagem de DHCP para pacotes que cruzam saltos da camada 3

Contents

Introdução

Este documento descreve as interações de rastreamento de DHCP e o comportamento quando o pacote está cruzando qualquer dispositivo L3 e se o pacote está encapsulado no cabeçalho L3.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Proficiência do Cisco IOS® XE em comandos operacionais e de configuração.
- Familiaridade com o hardware e a arquitetura do switch Cisco Catalyst série 9000.
- Uma sólida compreensão das operações do protocolo DHCP e dos mecanismos de rastreamento de DHCP.
- Compreensão conceitual da opção 82 do DHCP e da função do agente de retransmissão.
- Conhecimento básico do protocolo de roteamento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

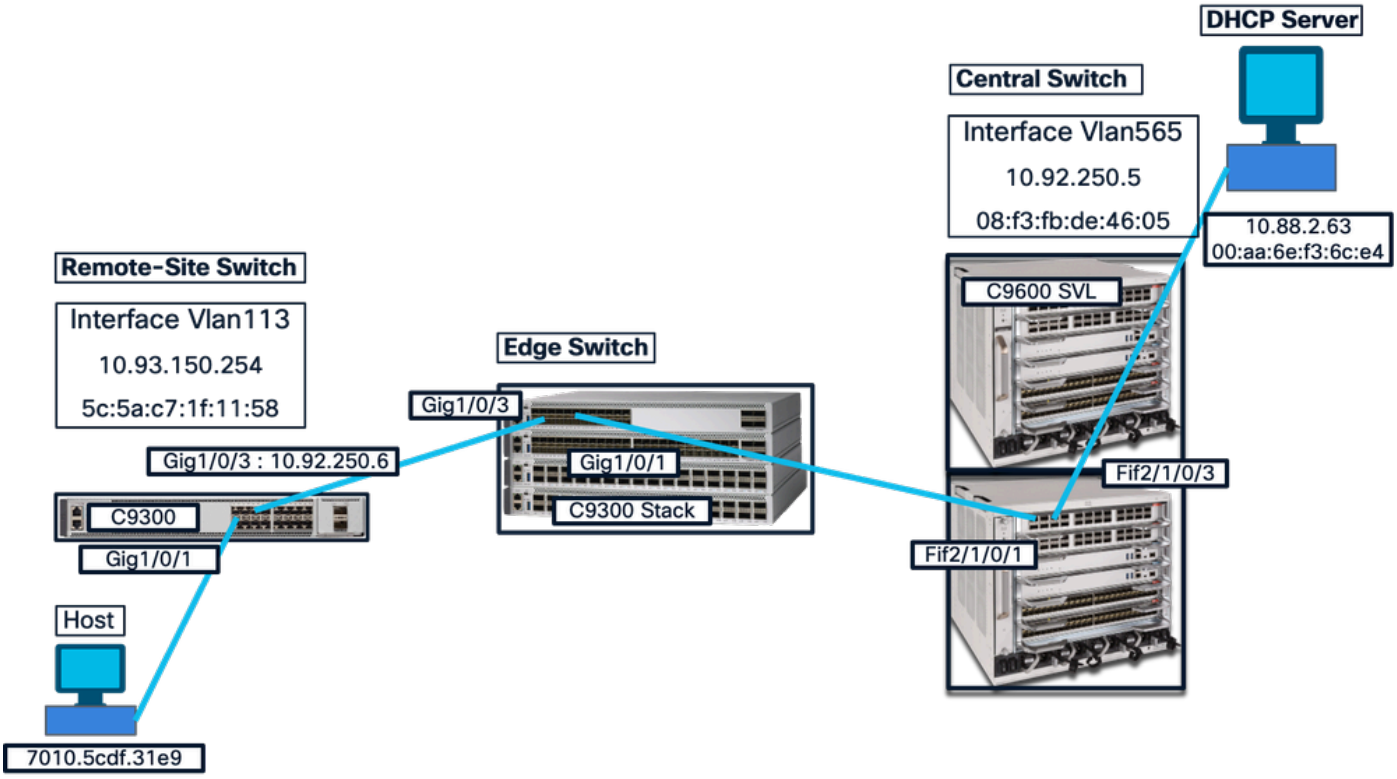
- Switch de núcleo/distribuição: Cisco Catalyst série 9600X
- Switch de acesso: Cisco Catalyst 9300 Series
- Cliente DHCP: Dispositivo de host final
- Servidor DHCP: Provedor de serviços de rede centralizado

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Este documento examina como o rastreamento de DHCP inspeciona e intercepta pacotes DHCP à medida que eles atravessam um salto de Camada 3. Usando exemplos práticos de configuração e análise de capturas de pacotes relacionados, ele demonstra a interação do rastreamento de DHCP nos saltos da Camada 3 dentro de um ambiente de rede da série Cisco Catalyst 9000.

Diagrama de Rede



Topologia

Cenário não funcional

Primeiro, o cenário em que o pacote DHCP Discover é descartado no salto da Camada 3 é descrito, especificamente no Switch Central. Agora, analise a jornada do pacote salto a salto a partir do cliente DHCP.

Processamento de Pacote de Switch de Site Remoto

O Host com endereço MAC 7010.5cdf.31e9 transmite o pacote DHCP Discover, que chega à interface GigabitEthernet1/0/1 no switch de local remoto.

Configuração de local remoto

<#root>

!
!

Remote-Site#show run int vlan 113

```
Building configuration...

Current configuration : 170 bytes
!
interface Vlan113
ip address 10.93.150.254 255.255.255.0
ip helper-address 10.88.2.63
no ip redirects
no ip proxy-arp
end
!
!
!
```

Host Access Port

Remote-Site#show run int gig1/0/1

```
Building configuration...

Current configuration : 90 bytes
!
interface GigabitEthernet1/0/1
switchport access vlan 113
switchport mode access
end
!
!
!
```

Uplink Port

Remote-Site#show run int gig1/0/3

```
Building configuration...

Current configuration : 121 bytes
!
interface GigabitEthernet1/0/3
no switchport
ip address 10.92.250.6 255.255.255.252
end
!
!
```

Remote-Site#show run | sec dhcp

```
ip dhcp snooping vlan 1-999
no ip dhcp snooping information option
```

```
ip dhcp snooping
!
!
```

Remote-Site#show cdp neighbors

```
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID     Local Intrfce    Holdtme      Capability    Platform       Port ID

Edge-Switch   Gig 1/0/3        153          R S I         C9300-48H      Gig 1/0/3
!
!
```

Remote-Site#show ip eigrp neighbors

```
EIGRP-IPv4 Neighbors for AS(100)
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
0 10.92.250.5 Gi1/0/3 14 00:04:40 1 100 0 20
!
!
```

Remote-Site#show ip route 10.88.2.63

```
Routing entry for 10.88.2.0/24
 Known via "eigrp 100", distance 90, metric 3072, precedence routine (0), type internal
 Redistributing via eigrp 100
 Last update from 10.92.250.5 on GigabitEthernet1/0/3, 00:05:15 ago
 Routing Descriptor Blocks:
 * 10.92.250.5, from 10.92.250.5, 00:05:15 ago, via GigabitEthernet1/0/3
     Route metric is 3072, traffic share count is 1
     Total delay is 20 microseconds, minimum bandwidth is 1000000 Kbit
     Reliability 255/255, minimum MTU 1500 bytes
     Loading 1/255, Hops 1
!
!
```

Entrada de switch de local remoto

O Pacote de Descoberta de DHCP de Broadcast está entrando no switch do local remoto.

<#root>

```
!
!
```

Remote-Site#show monitor capture tac parameter

```
     monitor capture tac control-plane BOTH
     monitor capture tac interface GigabitEthernet1/0/1 BOTH
     monitor capture tac match any
     monitor capture tac file location flash:pcport.pcap
!
!
```

Remote-Site#show monitor capture file flash:pcport.pcap packet-number 667 detailed

```
Starting the packet display ........ Press Ctrl + Shift + 6 to exit

Frame 667: 345 bytes on wire (2760 bits), 345 bytes captured (2760 bits) on interface 0
~
~
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:udp:bootp]
```

Ethernet II, Src: 70:10:5c:df:31:e9 (70:10:5c:df:31:e9), Dst: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)

```
Destination: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
Address: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
.... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
.... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
Source: 70:10:5c:df:31:e9 (70:10:5c:df:31:e9)
Address: 70:10:5c:df:31:e9 (70:10:5c:df:31:e9)
.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
.... ...0 .... .... .... .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
```

Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255

```
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 331
Identification: 0x0405 (1029)
Flags: 0x0000
0... .... .... .... = Reserved bit: Not set
.0.. .... .... .... = Don't fragment: Not set
..0. .... .... .... = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 255
```

Protocol: UDP (17)

```
Header checksum: 0xb69d [validation disabled]
[Header checksum status: Unverified]
Source: 0.0.0.0
Destination: 255.255.255.255
User Datagram Protocol, Src Port: 68, Dst Port: 67
```

Source Port: 68
Destination Port: 67
Length: 311
Checksum: 0x33de [unverified]
[Checksum Status: Unverified]
[Stream index: 3]
Bootstrap Protocol (Discover)
Message type: Boot Request (1)
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 0
Transaction ID: 0x000026ee
Seconds elapsed: 0
Bootp flags: 0x8000, Broadcast flag (Broadcast)
1... .... = Broadcast flag: Broadcast
.000 0000 0000 0000 = Reserved flags: 0x0000
Client IP address: 0.0.0.0
Your (client) IP address: 0.0.0.0
Next server IP address: 0.0.0.0
Relay agent IP address: 0.0.0.0

Client MAC address: 70:10:5c:df:31:e9 (70:10:5c:df:31:e9)

Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP

Option: (53) DHCP Message Type (Discover)

Length: 1
DHCP: Discover (1)
Option: (57) Maximum DHCP Message Size
Length: 2
Maximum DHCP Message Size: 1200
Option: (61) Client identifier
Length: 29
Type: 0
Client Identifier: cisco-7010.5cdf.31e9-Gi2/0/7
Option: (12) Host Name
Length: 2
Host Name: PC
Option: (55) Parameter Request List
Length: 8
Parameter Request List Item: (1) Subnet Mask
Parameter Request List Item: (6) Domain Name Server
Parameter Request List Item: (15) Domain Name
Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
Parameter Request List Item: (3) Router
Parameter Request List Item: (33) Static Route
Parameter Request List Item: (150) TFTP Server Address
Parameter Request List Item: (43) Vendor-Specific Information
Option: (60) Vendor class identifier
Length: 8
Vendor class identifier: ciscopnp
Option: (255) End
Option End: 255
!

```
!
```

Saída de switch de local remoto

O Pacote de Descoberta DHCP Unicast Retransmitido saindo do switch de local remoto para o Switch de Borda.

<#root>

```
!
!

Remote-Site#show monitor capture tac1 parameter


 monitor capture tac1 control-plane BOTH
 monitor capture tac1 interface GigabitEthernet1/0/3 BOTH
 monitor capture tac1 match any
 monitor capture tac1 file location flash:remote_edge.pcap
!
!

Remote-Site#show monitor capture file flash:pcport.pcap packet-number 669 detailed


Starting the packet display ........ Press Ctrl + Shift + 6 to exit

Frame 669: 345 bytes on wire (2760 bits), 345 bytes captured (2760 bits) on interface 0
~
~
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:udp:bootp]

Ethernet II, Src: 5c:5a:c7:1f:11:58 (5c:5a:c7:1f:11:58), Dst: 08:f3:fb:de:46:05 (08:f3:fb:de:46:05)


Destination: 08:f3:fb:de:46:05 (08:f3:fb:de:46:05)
Address: 08:f3:fb:de:46:05 (08:f3:fb:de:46:05)
.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
.... ...0 .... .... .... .... = IG bit: Individual address (unicast)
Source: 5c:5a:c7:1f:11:58 (5c:5a:c7:1f:11:58)
Address: 5c:5a:c7:1f:11:58 (5c:5a:c7:1f:11:58)
.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
.... ...0 .... .... .... .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 10.93.150.254, Dst: 10.88.2.63


0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
```

```
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 331
Identification: 0x001c (28)
Flags: 0x0000
0... .... .... .... = Reserved bit: Not set
.0.. .... .... .... = Don't fragment: Not set
..0. .... .... .... = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 255
Protocol: UDP (17)
Header checksum: 0x0c94 [validation disabled]
[Header checksum status: Unverified]
Source: 10.93.150.254
Destination: 10.88.2.63
User Datagram Protocol, Src Port: 67, Dst Port: 67
Source Port: 67
Destination Port: 67
Length: 311
Checksum: 0xe48f [unverified]
[Checksum Status: Unverified]
[Stream index: 4]
Bootstrap Protocol (Discover)
Message type: Boot Request (1)
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 1
Transaction ID: 0x000026ee
Seconds elapsed: 0
Bootp flags: 0x8000, Broadcast flag (Broadcast)
1... .... .... .... = Broadcast flag: Broadcast
.000 0000 0000 0000 = Reserved flags: 0x0000
Client IP address: 0.0.0.0
Your (client) IP address: 0.0.0.0
Next server IP address: 0.0.0.0
```

Relay agent IP address: 10.93.150.254

```
Client MAC address: 70:10:5c:df:31:e9 (70:10:5c:df:31:e9)
Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
```

Option: (53) DHCP Message Type (Discover)

```
Length: 1
DHCP: Discover (1)
Option: (57) Maximum DHCP Message Size
Length: 2
Maximum DHCP Message Size: 1200
Option: (61) Client identifier
Length: 29
Type: 0
Client Identifier: cisco-7010.5cdf.31e9-Gi2/0/7
Option: (12) Host Name
Length: 2
```

```
Host Name: PC
Option: (55) Parameter Request List
Length: 8
Parameter Request List Item: (1) Subnet Mask
Parameter Request List Item: (6) Domain Name Server
Parameter Request List Item: (15) Domain Name
Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
Parameter Request List Item: (3) Router
Parameter Request List Item: (33) Static Route
Parameter Request List Item: (150) TFTP Server Address
Parameter Request List Item: (43) Vendor-Specific Information
Option: (60) Vendor class identifier
Length: 8
Vendor class identifier: ciscopnp
Option: (255) End
Option End: 255
!
!
```

Note: O pacote tem o 'Endereço IP do agente de retransmissão: 10.93.150.254', mas não tem a Opção de DHCP 82 devido à configuração 'no ip dhcp snooping information option' como parte da seção DHCP.

Processamento de Pacote de Switch de Borda

Para o fluxo DHCP ser uma preocupação, o switch de borda é um switch L2 usado apenas para distribuir os pacotes de e para entre o switch central/central e os switches de local remoto. Ele confia em todos os pacotes DHCP.

Configuração do switch de borda

<#root>

```
!
!
```

Edge-Switch#show run int gig1/0/3

```
Building configuration...

Current configuration : 152 bytes
!
interface GigabitEthernet1/0/3
switchport access vlan 565
ip flow monitor IPv4_NETFLOW input
ip dhcp snooping trust
end
```

```
!
!
```

Edge-Switch#show run int gig1/0/1

```
Building configuration...

Current configuration : 119 bytes
!
interface GigabitEthernet1/0/1
switchport trunk native vlan 999
switchport mode trunk
ip dhcp snooping trust
end
!
!
```

Edge-Switch#show run | sec dhcp

```
ip dhcp snooping vlan 1-4094
no ip dhcp snooping information option
ip dhcp snooping
!
!
```

Edge-Switch#show cdp neighbors

```
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce   Holdtme   Capability   Platform     Port ID
Remote-Site      Gig 1/0/3       153       R S I        C9300L-48    Gig 1/0/3
Central-Switch   Gig 1/0/1       170       R S I        C9606R       Fif 2/1/0/1
!
!
```

Entrada de switch de borda

O pacote que sai do Switch de local remoto está atingindo o Switch de borda da rede como ele está.

Saída do switch de borda

Como esse é um salto de Camada 2 para o pacote, ele sai do switch inalterado enquanto avança para o próximo salto. O switch de borda encaminha o pacote ao switch central sem qualquer modificação observada no pacote.

Edge Switch Egress Packet é um pacote de entrada do switch central.

<#root>

```
!
!

Edge-Switch#show monitor capture tac parameters


 monitor capture tac control-plane BOTH
 monitor capture tac interface GigabitEthernet1/0/1 BOTH
 monitor capture tac match any
 monitor capture tac file location flash:edge_central.pcap
!
!

Edge-Switch#show monitor capture file flash:edge_central.pcap packet-number 25597 detail


Starting the packet display ........ Press Ctrl + Shift + 6 to exit

Frame 25597: 345 bytes on wire (2760 bits), 345 bytes captured (2760 bits) on interface /tmp/epc_ws/wif
~
~
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:udp:dhcp]

Ethernet II, Src: 5c:5a:c7:1f:11:58 (5c:5a:c7:1f:11:58), Dst: 08:f3:fb:de:46:05 (08:f3:fb:de:46:05)


Destination: 08:f3:fb:de:46:05 (08:f3:fb:de:46:05)
Address: 08:f3:fb:de:46:05 (08:f3:fb:de:46:05)
.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
.... ...0 .... .... .... .... = IG bit: Individual address (unicast)
Source: 5c:5a:c7:1f:11:58 (5c:5a:c7:1f:11:58)
Address: 5c:5a:c7:1f:11:58 (5c:5a:c7:1f:11:58)
.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
.... ...0 .... .... .... .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 10.93.150.254, Dst: 10.88.2.63


0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 331
Identification: 0x001c (28)
Flags: 0x0000
0... .... .... .... = Reserved bit: Not set
.0.. .... .... .... = Don't fragment: Not set
..0. .... .... .... = More fragments: Not set
```

Fragment offset: 0
Time to live: 255

Protocol: UDP (17)

Header checksum: 0x0c94 [validation disabled]
[Header checksum status: Unverified]
Source: 10.93.150.254
Destination: 10.88.2.63
User Datagram Protocol, Src Port: 67, Dst Port: 67
Source Port: 67
Destination Port: 67
Length: 311
Checksum: 0xe48f [unverified]
[Checksum Status: Unverified]
[Stream index: 5]
[Timestamps]
[Time since first frame: 0.000000000 seconds]
[Time since previous frame: 0.000000000 seconds]

Dynamic Host Configuration Protocol (Discover)

Message type: Boot Request (1)
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 1
Transaction ID: 0x000026ee
Seconds elapsed: 0
Bootp flags: 0x8000, Broadcast flag (Broadcast)
1... .... = Broadcast flag: Broadcast
.000 0000 0000 0000 = Reserved flags: 0x0000
Client IP address: 0.0.0.0
Your (client) IP address: 0.0.0.0
Next server IP address: 0.0.0.0

Relay agent IP address: 10.93.150.254

Client MAC address: 70:10:5c:df:31:e9 (70:10:5c:df:31:e9)
Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
Option: (53) DHCP Message Type (Discover)
Length: 1
DHCP: Discover (1)
Option: (57) Maximum DHCP Message Size
Length: 2
Maximum DHCP Message Size: 1200
Option: (61) Client identifier
Length: 29
Type: 0
Client Identifier: cisco-7010.5cdf.31e9-Gi2/0/7
Option: (12) Host Name
Length: 2
Host Name: PC
Option: (55) Parameter Request List

```
Length: 8
Parameter Request List Item: (1) Subnet Mask
Parameter Request List Item: (6) Domain Name Server
Parameter Request List Item: (15) Domain Name
Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
Parameter Request List Item: (3) Router
Parameter Request List Item: (33) Static Route
Parameter Request List Item: (150) TFTP Server Address
Parameter Request List Item: (43) Vendor-Specific Information
Option: (60) Vendor class identifier
Length: 8
Vendor class identifier: ciscopnp
Option: (255) End
Option End: 255
!
!
```

Processamento de Pacote de Switch Central

Configuração do Switch Central

<#root>

```
!
!

Central-Switch#show cdp neighbors


Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID      Local Intrfce   Holdtme   Capability   Platform    Port ID

Edge-Switch    Fif 2/1/0/1     177       R S I        C9300-48H   Gig 1/0/1
!
!

Central-Switch#show run int fif2/1/0/1


Building configuration...

Current configuration : 115 bytes
!
interface FiftyGigE2/1/0/1
switchport trunk native vlan 999
switchport mode trunk
end
!
!
```

Central-Switch#show run int fif2/1/0/3

Building configuration...

Current configuration : 87 bytes
!
interface FiftyGigE2/1/0/3
no switchport
ip address 10.88.2.254 255.255.255.0
end
!
!

interface Vlan565

ip address 10.92.250.5 255.255.255.252
!
!
!

Central-Switch#show run | sec dhcp

ip dhcp snooping vlan 1-4094
no ip dhcp snooping information option
ip dhcp snooping
!
!

Central-Switch#show ip eigrp neighbors

EIGRP-IPv4 Neighbors for AS(100)
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
0

10.92.250.6

Vl565 11 00:10:32 3 100 0 19
~
~
!
!

router eigrp 100

  network 10.0.0.0
  network 10.88.0.0 0.0.255.255
  passive-interface default
  no passive-interface Vlan565
  eigrp router-id 10.255.255.254
!
!

Entrada de switch central

Como mencionado anteriormente, o Pacote de saída do switch de borda é um pacote de entrada do switch central.

Quando o pacote chega à interface fif 2/1/0/1, esse registro é observado.

```
%DHCP_SNOOPING-5-DHCP_SNOOPING_NONZERO_GIADDR: DHCP_SNOOPING drop message with non-zero giaddr or optio
```

A interface Fif 2/1/0/1 está configurada como uma porta não confiável para rastreamento de DHCP.

Um pacote DHCP Discover retransmitido de Camada 3 entra por essa porta. Embora o pacote seja retransmitido e encapsulado na Camada 3, o rastreamento de DHCP ainda o inspeciona na porta da Camada 2. Como essa porta não é confiável e o pacote contém um endereço IP de gateway (agente de retransmissão) sem a opção 82, o rastreamento de DHCP descartará o pacote nessa porta não confiável. Esse comportamento é esperado e planejado.

Note: Em muitos dos casos, observa-se que a descoberta de DHCP é descartada em trânsito devido à espionagem de DHCP.

Saída do switch central

Nesse caso, o switch central descartará o pacote DHCP Discover e não haverá nenhum pacote DHCP Discover iniciado pelo host com endereço MAC 70:10:5c:df:31:e9 saindo da interface Fif 2/1/0/3.

Como corrigir o problema?

1. Tenha a Opção 82 ativada no primeiro salto do cliente DHCP.
No exemplo atual, configure o comando ip dhcp snooping information option no Switch Remoto.

2. A relação de confiança de rastreamento de DHCP deve ser habilitada em todo o caminho DHCP do cliente DHCP para o servidor DHCP.

No exemplo atual, configure o comando ip dhcp snooping trust na interface fif2/1/0/1 do Switch Central.

<#root>

Central-Switch#show run int fif2/1/0/1

```
Building configuration...

Current configuration : 115 bytes
!
interface FiftyGigE2/1/0/1
switchport trunk native vlan 999
switchport mode trunk
```

ip dhcp snooping trust

```
end
```

Após essas alterações, o pacote Discover começará a sair do switch central para o servidor DHCP.

<#root>

Frame 9: 345 bytes on wire (2760 bits), 345 bytes captured (2760 bits) on interface 0

```
~
~
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:udp:dhcp]
```

Ethernet II, Src: 08:f3:fb:de:46:05 (08:f3:fb:de:46:05), Dst: 00:aa:6e:f3:6c:e4 (00:aa:6e:f3:6c:e4)

```
Destination: 00:aa:6e:f3:6c:e4 (00:aa:6e:f3:6c:e4)
Address: 00:aa:6e:f3:6c:e4 (00:aa:6e:f3:6c:e4)
.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
.... ...0 .... .... .... .... = IG bit: Individual address (unicast)
Source: 08:f3:fb:de:46:05 (08:f3:fb:de:46:05)
Address: 08:f3:fb:de:46:05 (08:f3:fb:de:46:05)
.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
.... ...0 .... .... .... .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
```

Internet Protocol Version 4, Src: 10.93.150.254, Dst: 10.88.2.63

0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 331
Identification: 0x02ff (767)
Flags: 0x0000
0... .... = Reserved bit: Not set
.0.. .... = Don't fragment: Not set
..0. .... = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 254
Protocol: UDP (17)
Header checksum: 0x0ab1 [validation disabled]
[Header checksum status: Unverified]
Source: 10.93.150.254
Destination: 10.88.2.63
User Datagram Protocol, Src Port: 67, Dst Port: 67
Source Port: 67
Destination Port: 67
Length: 311
Checksum: 0x061b [unverified]
[Checksum Status: Unverified]
[Stream index: 0]
[Timestamps]
[Time since first frame: 0.000000000 seconds]
[Time since previous frame: 0.000000000 seconds]

Dynamic Host Configuration Protocol (Discover)

Message type: Boot Request (1)
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 1
Transaction ID: 0x00000563
Seconds elapsed: 0
Bootp flags: 0x8000, Broadcast flag (Broadcast)
1... .... = Broadcast flag: Broadcast
.000 0000 0000 0000 = Reserved flags: 0x0000
Client IP address: 0.0.0.0
Your (client) IP address: 0.0.0.0
Next server IP address: 0.0.0.0
Relay agent IP address: 10.93.150.254

Client MAC address: 70:10:5c:df:31:e9 (70:10:5c:df:31:e9)

Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
Option: (53) DHCP Message Type (Discover)
Length: 1
DHCP: Discover (1)
Option: (57) Maximum DHCP Message Size
Length: 2
Maximum DHCP Message Size: 1200

```
Option: (61) Client identifier
Length: 29
Type: 0
Client Identifier: cisco-7010.5cdf.31e9-Gi2/0/7
Option: (12) Host Name
Length: 2
Host Name: PC
Option: (55) Parameter Request List
Length: 8
Parameter Request List Item: (1) Subnet Mask
Parameter Request List Item: (6) Domain Name Server
Parameter Request List Item: (15) Domain Name
Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
Parameter Request List Item: (3) Router
Parameter Request List Item: (33) Static Route
Parameter Request List Item: (150) TFTP Server Address
Parameter Request List Item: (43) Vendor-Specific Information
Option: (60) Vendor class identifier
Length: 8
Vendor class identifier: ciscopnp
Option: (255) End
Option End: 255
```

A Descoberta alcançará o servidor DHCP e o servidor DHCP responderá a oferta DHCP.

Pacote de oferta DHCP:

<#root>

Frame 128: 353 bytes on wire (2824 bits), 353 bytes captured (2824 bits) on interface 0

```
~
~
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:udp:bootp]
```

Ethernet II, Src: 00:aa:6e:f3:6c:e4 (00:aa:6e:f3:6c:e4), Dst: 08:f3:fb:de:46:05 (08:f3:fb:de:46:05)

```
Destination: 08:f3:fb:de:46:05 (08:f3:fb:de:46:05)
Address: 08:f3:fb:de:46:05 (5c:5a:c7:1f:11:58)
.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
.... ...0 .... .... .... .... = IG bit: Individual address (unicast)
Source: 00:aa:6e:f3:6c:e4 (00:aa:6e:f3:6c:e4)
Address: 00:aa:6e:f3:6c:e4 (00:aa:6e:f3:6c:e4)
.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
.... ...0 .... .... .... .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
```

Internet Protocol Version 4, Src: 10.88.2.63, Dst: 10.93.150.254

0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 339
Identification: 0x0006 (6)
Flags: 0x0000
0... .... = Reserved bit: Not set
.0.. .... = Don't fragment: Not set
..0. .... = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 252
Protocol: UDP (17)
Header checksum: 0x0fa2 [validation disabled]
[Header checksum status: Unverified]
Source: 10.88.2.63
Destination: 10.93.150.254
User Datagram Protocol, Src Port: 67, Dst Port: 67
Source Port: 67
Destination Port: 67
Length: 319
Checksum: 0x9c4c [unverified]
[Checksum Status: Unverified]
[Stream index: 2]
Bootstrap Protocol (Offer)
Message type: Boot Reply (2)
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 0
Transaction ID: 0x00000563
Seconds elapsed: 0
Bootp flags: 0x8000, Broadcast flag (Broadcast)
1... .... = Broadcast flag: Broadcast
.000 0000 0000 0000 = Reserved flags: 0x0000
Client IP address: 0.0.0.0

Your (client) IP address: 10.93.150.11

Next server IP address: 0.0.0.0

Relay agent IP address: 10.93.150.254

Client MAC address: 70:10:5c:df:31:e9 (70:10:5c:df:31:e9)

Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP

Option: (53) DHCP Message Type (Offer)

```
Length: 1
DHCP: Offer (2)
Option: (61) Client identifier
Length: 29
Type: 0
Client Identifier: cisco-7010.5cdf.31e9-Gi2/0/7
Option: (54) DHCP Server Identifier
Length: 4
```

DHCP Server Identifier: 10.88.2.63

```
Option: (51) IP Address Lease Time
Length: 4
IP Address Lease Time: (73119s) 20 hours, 18 minutes, 39 seconds
Option: (58) Renewal Time Value
Length: 4
Renewal Time Value: (36559s) 10 hours, 9 minutes, 19 seconds
Option: (59) Rebinding Time Value
Length: 4
Rebinding Time Value: (63973s) 17 hours, 46 minutes, 13 seconds
Option: (1) Subnet Mask
Length: 4
Subnet Mask: 255.255.255.0
Option: (6) Domain Name Server
Length: 4
Domain Name Server: 8.8.8.8
Option: (255) End
Option End: 255
```

O pacote Offer respondido de volta pelo servidor DHCP atingirá a interface fif2/1/0/3 do switch CORE/Central.

<#root>

Central-Switch#show run int fif2/1/0/3

```
Building configuration...

Current configuration : 87 bytes
!
interface FiftyGigE2/1/0/3
no switchport
ip address 10.88.2.254 255.255.255.0
end
```

Aqui não há confiança do DHCP snooping end e OFFER está entrando, então por que a oferta não está sendo descartada em uma porta não confiável?

Como você sabe, em uma rede onde o rastreamento de DHCP está habilitado, as portas são categorizadas como confiáveis ou não confiáveis.

As portas confiáveis são conectadas a servidores DHCP legítimos ou a outros switches confiáveis. Todas as mensagens DHCP são permitidas.
As portas não confiáveis normalmente são conectadas a dispositivos de usuário final (clientes). Eles são restritos para evitar ataques de "DHCP Spoofing" ou "Rogue DHCP Server".
Os pacotes DHCP Offer e DHCP ACK são considerados mensagens do lado do servidor. De acordo com as regras de segurança, essas mensagens só devem se originar de um servidor legítimo.
Quando um agente de retransmissão DHCP ou qualquer Roteador/Switch L3 recebe uma oferta DHCP em uma porta L2 configurada como não confiável, o mecanismo de rastreamento de DHCP identifica isso como uma violação de segurança. Pressupõe-se que um servidor DHCP invasor esteja tentando fornecer endereços IP não autorizados aos clientes na rede.
Mesmo que o pacote seja unicast (direcionado especificamente para o agente de retransmissão), o estado de confiança da porta física ou lógica tem precedência. A verificação de segurança é executada no nível da porta, independentemente de o pacote ser broadcast ou unicast.
Como a porta não é confiável, o sistema bloqueará a Oferta DHCP para proteger a rede de dados de configuração potencialmente mal-intencionados ou incorretos provenientes de uma fonte não autorizada.

Uma porta L3 (uma interface roteada) opera na Camada 3. Por ser uma interface roteada, ela não observa as regras de confiança/não confiança de rastreamento de DHCP da L2 que se aplicam às portas de switch.
Um cliente envia uma solicitação de broadcast. O Agente de Retransmissão (o dispositivo L3) intercepta isso e envia uma solicitação unicast ao servidor DHCP.
O servidor DHCP envia uma oferta DHCP unicast de volta para o endereço IP do agente de retransmissão (especificamente para o endereço IP do gateway ou giaddr).
Quando o pacote chega à porta L3 do Agente de Retransmissão ou em qualquer salto L3 no caminho do pacote, o dispositivo aceita o pacote como tráfego de roteamento legítimo.
Ao contrário do cenário anterior (uma porta não confiável L2), em que o switch procura mensagens "do lado do servidor" vindas de uma porta voltada para o cliente, a porta L3 está agindo como o destino pretendido ou salto L3 legítimo para a resposta do servidor.
Se as portas L3 tiverem descartado as ofertas de DHCP unicast, o mecanismo de retransmissão de DHCP nunca funcionará, pois o servidor nunca poderá se comunicar de volta com o agente de retransmissão.

Finalmente, o pacote Offer passará até alcançar o cliente.

O host/cliente responderá com a solicitação DHCP.

Frame 20: 363 bytes on wire (2904 bits), 363 bytes captured (2904 bits) on interface 0

~
~
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:udp:bootp]

Ethernet II, Src: 70:10:5c:df:31:e9 (70:10:5c:df:31:e9), Dst: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)

Destination: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
Address: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
.... ..1. .... = LG bit: Locally administered address (this is NOT the factory default)
....1 .... = IG bit: Group address (multicast/broadcast)
Source: 70:10:5c:df:31:e9 (70:10:5c:df:31:e9)
Address: 70:10:5c:df:31:e9 (70:10:5c:df:31:e9)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255

0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 349
Identification: 0x3be5 (15333)
Flags: 0x0000
0... .... = Reserved bit: Not set
.0.. .... = Don't fragment: Not set
..0. .... = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 255
Protocol: UDP (17)
Header checksum: 0x7eab [validation disabled]
[Header checksum status: Unverified]
Source: 0.0.0.0
Destination: 255.255.255.255
User Datagram Protocol, Src Port: 68, Dst Port: 67
Source Port: 68
Destination Port: 67
Length: 329
Checksum: 0xed98 [unverified]
[Checksum Status: Unverified]
[Stream index: 1]
Bootstrap Protocol (Request)

Message type: Boot Request (1)

Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 0
Transaction ID: 0x00000563

Seconds elapsed: 0
Bootp flags: 0x8000, Broadcast flag (Broadcast)
1... .... = Broadcast flag: Broadcast
.000 0000 0000 0000 = Reserved flags: 0x0000
Client IP address: 0.0.0.0
Your (client) IP address: 0.0.0.0
Next server IP address: 0.0.0.0
Relay agent IP address: 0.0.0.0

Client MAC address: 70:10:5c:df:31:e9 (70:10:5c:df:31:e9)

Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP

Option: (53) DHCP Message Type (Request)

Length: 1
DHCP: Request (3)
Option: (57) Maximum DHCP Message Size
Length: 2
Maximum DHCP Message Size: 1200
Option: (61) Client identifier
Length: 29
Type: 0
Client Identifier: cisco-7010.5cdf.31e9-Gi2/0/7
Option: (54) DHCP Server Identifier
Length: 4

DHCP Server Identifier: 10.88.2.63

Option: (50) Requested IP Address
Length: 4

Requested IP Address: 10.93.150.11

Option: (51) IP Address Lease Time
Length: 4
IP Address Lease Time: (73119s) 20 hours, 18 minutes, 39 seconds
Option: (12) Host Name
Length: 2
Host Name: PC
Option: (55) Parameter Request List
Length: 8
Parameter Request List Item: (1) Subnet Mask
Parameter Request List Item: (6) Domain Name Server
Parameter Request List Item: (15) Domain Name
Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
Parameter Request List Item: (3) Router
Parameter Request List Item: (33) Static Route
Parameter Request List Item: (150) TFTP Server Address
Parameter Request List Item: (43) Vendor-Specific Information
Option: (60) Vendor class identifier

```
Length: 8
Vendor class identifier: ciscopnp
Option: (255) End
Option End: 255
```

O servidor DHCP finalmente confirmará a atribuição de endereço IP.

<#root>

Frame 25: 353 bytes on wire (2824 bits), 353 bytes captured (2824 bits) on interface 0

```
~
~
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:udp:bootp]
```

Ethernet II, Src: 08:f3:fb:de:46:05 (08:f3:fb:de:46:05), Dst: 5c:5a:c7:1f:11:58 (5c:5a:c7:1f:11:58)

```
Destination: 5c:5a:c7:1f:11:58 (5c:5a:c7:1f:11:58)
Address: 5c:5a:c7:1f:11:58 (5c:5a:c7:1f:11:58)
.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
.... ...0 .... .... .... .... = IG bit: Individual address (unicast)
Source: 08:f3:fb:de:46:05 (08:f3:fb:de:46:05)
Address: 08:f3:fb:de:46:05 (08:f3:fb:de:46:05)
.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
.... ...0 .... .... .... .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
```

Internet Protocol Version 4, Src: 10.88.2.63, Dst: 10.93.150.254

```
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
0000 00.. = Differentiated Services Codepoint: Default (0)
.... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
Total Length: 339
Identification: 0x0007 (7)
Flags: 0x0000
0... .... .... .... = Reserved bit: Not set
.0.. .... .... .... = Don't fragment: Not set
..0. .... .... .... = More fragments: Not set
...0 0000 0000 0000 = Fragment offset: 0
Time to live: 252
Protocol: UDP (17)
Header checksum: 0x0fa1 [validation disabled]
[Header checksum status: Unverified]
Source: 10.88.2.63
Destination: 10.93.150.254
User Datagram Protocol, Src Port: 67, Dst Port: 67
```

Source Port: 67
Destination Port: 67
Length: 319
Checksum: 0x1e0f [unverified]
[Checksum Status: Unverified]
[Stream index: 2]

Bootstrap Protocol (ACK)

Message type: Boot Reply (2)
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 0
Transaction ID: 0x00000563
Seconds elapsed: 0
Bootp flags: 0x8000, Broadcast flag (Broadcast)
1... .... = Broadcast flag: Broadcast
.000 0000 0000 0000 = Reserved flags: 0x0000
Client IP address: 0.0.0.0

Your (client) IP address: 10.93.150.11

Next server IP address: 0.0.0.0

Relay agent IP address: 10.93.150.254

Client MAC address: 70:10:5c:df:31:e9 (70:10:5c:df:31:e9)

Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP

Option: (53) DHCP Message Type (ACK)

Length: 1
DHCP: ACK (5)
Option: (61) Client identifier
Length: 29
Type: 0
Client Identifier: cisco-7010.5cdf.31e9-Gi2/0/7
Option: (54) DHCP Server Identifier
Length: 4

DHCP Server Identifier: 10.88.2.63

Option: (51) IP Address Lease Time
Length: 4
IP Address Lease Time: (86400s) 1 day

```
Option: (58) Renewal Time Value
Length: 4
Renewal Time Value: (43200s) 12 hours
Option: (59) Rebinding Time Value
Length: 4
Rebinding Time Value: (75600s) 21 hours
Option: (1) Subnet Mask
Length: 4
Subnet Mask: 255.255.255.0
Option: (6) Domain Name Server
Length: 4
Domain Name Server: 8.8.8.8
Option: (255) End
Option End: 255
```

O DORA é concluído e o host receberá o endereço IP com êxito.

Summary

Consulte esta tabela para entender os cenários de encaminhamento de pacotes.

Tipo de porta	Estado de Confiança	Tipo de pacote retransmitido	Resultado	Razão
Porta L2	Não confiável	Oferta/confirmação de DHCP unicast	Descartado	O DHCP Snooping impede mensagens do servidor em portas L2 não confiáveis.
Porta L3	N/D (Roteado)	Oferta/confirmação de DHCP unicast	Aceito	As portas roteadas são os nós desejados para a comunicação do agente de retransmissão.
Porta L2	Confiável	Descoberta DHCP Unicast com opção 82	Aceito	A porta confiável permite todos os sinais DHCP.
Porta L2	Não confiável	Descoberta DHCP Unicast com opção 82	Aceito	O pacote com o endereço IP do agente de retransmissão e a Opção 82 é legítimo.
Porta L2	Confiável	Descoberta DHCP Unicast sem opção 82	Aceito	A porta confiável permite todos os sinais DHCP.

Porta L2	Não confiável	Descoberta DHCP Unicast sem opção 82	Descartado	O pacote com endereço IP do agente de retransmissão e nenhuma opção 82 é invasor.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.